Claims

1. A method (400, 500, 600, 700) for synchronizing state information in a security gateway cluster, said security gateway cluster comprising at least two nodes, said method comprising the step of:
- synchronizing (403) state information by sending state information from a first node of said at least two nodes,
characterized in that it comprises the steps of:
- detecting (401) in said security gateway cluster a predetermined irregularly occurring action, and
- initiating (402) synchronization of state information as a response to said action,
and in that in said step of synchronizing state information, state information is sent to at least a second node of said at least two nodes.

2. A method according to claim 1, **characterized** in that said predetermined action is modification of state information (602) stored in said first node.

3. A method according to claim 2, **characterized** in that in the step of synchronizing state information only modified part of the state information stored in said first node is sent.

4. A method according to claim 3, **characterized** in that the modified part of the state information is sent from said first node to all other nodes of said security gateway cluster.

5. A method according to claim 4, **characterized** in that the modified part of the state information relates to a certain protocol, authentication information, virtual private network parameters or intrusion detection system.

6. A method according to claim 1, **characterized** in that in the step of synchronizing state information all state information stored in said first node is sent.

7. A method (500) according to claim 1, **characterized** in that it further comprises the step of:
- periodically synchronizing (501, 403) state information from said first node to at least a second node.

8. A method (600) according to claim 1, **characterized** in that it further comprises the step of:

- defining (601) for each node belonging to said security gateway cluster a node-specific backup group comprising at least one node-specific backup node,
and in that when a node initiates synchronizing of state information, state information is sent (605) at least to nodes belonging to a respective node-specific backup group.

9. A method according to claim 8, **characterized** in that
- state information stored in said first node comprises common state information and node-specific state information,
- modification of common state information initiates synchronization (604) of common state information to all other nodes of said security gateway cluster, and
- modification of node-specific state information initiates synchronization (605) of node-specific state information to nodes belonging to backup group of said first node.

10. A method according to claim 9, **characterized** in that said predetermined action affects number of nodes in said security gateway cluster and in that said method further comprises the step of:
- redefining (703) for at least one node belonging to said security gateway cluster a backup group comprising at least one backup node.

11. A method (700) according to claim 1, **characterized** in that said predetermined action is said first node failing (701) to continue normal operation.

12. A method according to claim 1, **characterized** in that said predetermined action is said second node requesting (704) for state information.

13. A method according to claim 1, **characterized** in that said predetermined action is said first node initiating a transition to offline state.

14. A method according to claim 1, **characterized** in that said predetermined action is handling of data packets relating to a communication session in at least two nodes, one of them being said first node, and in that said synchronization of state information is performed between at least said at least two nodes.

15. A method (800) according to claim 1, **characterized** in that said predetermined action is a receipt (801) of a data packet in said first node of said security gateway cluster, said data packet relating to a command to open a new connection via said security gateway cluster.

16. A method according to claim 15, **characterized** in that it further comprises the step of:
- delaying (803) sending of said data packet from said first node until said synchronization of state information is performed.

17. A method according to claim 1, **characterized** in that it further comprises the step of:
- delaying sending of a plurality of data packets from said first node until said synchronization of state information is performed.

18. A computer program comprising program code for performing all the steps of Claim 1 when said program is run on a computer.

19. A computer program product comprising program code means stored on a computer readable medium for performing the method of Claim 1 when said program product is run on a computer.

20. A first software entity (910) for a node (900) in a security gateway cluster, said first software entity comprising
- program code means (911) for processing data packets,
- program code means (912) for storing state information of said node,
and
- program code means (914) for synchronizing said state information with at least a second first software entity in one other node of said security gateway cluster,
characterized in that said first software entity further comprises
- program code means (915) for receiving from said second software entity instructions to initiate synchronizing said state information,
and in that said program code means (914) for synchronizing said state information are arranged to initiate synchronization as a response to receipt of instructions to initiate synchronization.

21. A first software entity according to claim 20, **characterized** in that it further comprises
- program code means (916) for causing a data packet to be delayed until an initiated state information synchronization is complete.

22. A first software entity according to claim 21, **characterized** in that said program code means (916) for causing a data packet to be delayed are arranged to delay said data packet.

23. A first software entity according to claim 21, **characterized** in that said program code means (916) for causing a data packet to be delayed are arranged to inform the second software entity when an initiated state information synchronization is complete.

24. A first software entity according to claim 20, **characterized** in that it further comprises
- program code means (913) for receiving instructions to modify said state information from a second software entity residing in a same node as said first software entity.

25. A second software entity (920) for a node in a security gateway cluster, said second software entity comprising
- program code means (921) for monitoring data packets relating to certain communication protocol connections,
characterized in that it further comprises
- program code means (923) for delivering to a first software entity instructions to initiate synchronizing said state information.

26. A second software entity according to claim 25, **characterized** in that it further comprises
- program code means (924) for causing a data packet to be delayed until an initiated state information synchronization is complete.

27. A second software entity according to claim 26, **characterized** in that said program code means (924) for causing a data packet to be delayed are arranged to inform the first software entity to delay a data packet.

28. A second software entity according to claim 26, **characterized** in that said program code means (924) for causing a data packet to be delayed are arranged to be informed by the first software entity, when an initiated state information synchronization is complete, and subsequently trigger delivery of said data packet to the first software entity.

29. A second software entity according to claim 25, **characterized** in that it further comprises
- program code means (922) for delivering to a first software entity instructions to modify state information comprising information about connections.

30. A node (900) of a security gateway cluster comprising

- means (931) for storing state information of said node, and
- means (932) for synchronizing said state information with at least one other node of said security gateway cluster,
characterized in that it further comprises
- means (933) for detecting a predetermined irregularly occurring action, and
- means (934) for initiating synchronization of said state information as a response to said irregularly occurring action.

31. A security gateway cluster (950) having a plurality of nodes (900a, 900b), at least one node comprising
- means (931) for storing state information of said node, and
- means (932) for synchronizing said state information with at least one other node of said security gateway cluster,
characterized in that said at least one node further comprises
- means (933) for detecting a predetermined irregularly occurring action, and
- means (934) for initiating synchronization of said state information as a response to said action.

32. A security gateway cluster (950) according to claim 31, **characterized** in that it further comprises
- means (951) for defining for said at least one node a node-specific backup group by selecting at least one node-specific backup node,
and in that said means (932) for synchronizing said state information with at least one other node of the security gateway cluster are arranged to synchronize said state information from said at least one node to respective node-specific backup group.